Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for protecting digital television from unauthorized digital receivers within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

at a broadcaster:

receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from ~~a~~ the broadcaster;

distributing first decryption information to the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

encrypting first content using a first method using a content encryption key;

distributing the first content;

encrypting the content encryption key using the first decryption information, the first decryption information being generated using the provisioning information; and

distributing the content encryption key to the subset of the population of digital receivers using a second decryption information, wherein the second

decryption information is cryptographically secured with the first decryption information.

2. (Previously presented) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising steps of:

encrypting second content using a second method that is cryptographically related to third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method;

sending the second content; and

distributing third decryption information to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information.

3. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of uniquely encrypting the first decryption information for each of the subset, wherein the first-listed distributing step comprises sending first description information uniquely encrypted for each of the subset.

4. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further

comprising a step of determining the unauthorized digital receivers to exclude from the subset of the population of digital receivers.

5. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information is uniquely encrypted for each of the subset.

6. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information comprises a key for decrypting the second decryption information.

7. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information expires by changing keys, key lengths and/or algorithms used to encrypt the first content.

8. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset.

9. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the unique identifier includes a key.

10. (Cancelled)

11. (Original) A computer system adapted to perform the computer-implementable method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 1.

12. (Previously presented) A method for processing digital television within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

at a subset of the population of digital receivers:

sending provisioning information from the subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster;

receiving first decryption information by the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

receiving first content;

receiving content encryption information from the broadcaster, wherein the content encryption information is encrypted using the first decryption information; and

decrypting the first content using the content encryption information,

wherein the first decryption information is based on the provisioning information.

13. (Previously Presented) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, further comprising steps of:

receiving second content;

receiving third decryption information from the broadcaster, wherein the third decryption information is cryptographically secured with the first decryption information; and

decrypting the second content using a second method that is cryptographically related to the third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method.

14. (Original) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the first decryption information is uniquely encrypted for each of the subset.

15. (Original) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the unique identifier includes a key.

16. (Canceled)

17. (Original) A computer system adapted to perform the computer-implementable method for processing digital television within the population of digital receivers of claim 12.

Claims 18-21 Canceled.

22. (Previously presented) A content receiver for protecting content that is transmitted with digital encoding, the content receiver comprising:

provisioning information that is sent away from the content receiver for a plurality of content broadcasters coupled to the content receiver;

first decryption information received from a point remote to the content receiver, wherein an unauthorized content receiver is excluded from using the first decryption information;

an interface coupled to content signals broadcast to a plurality of content receivers, wherein the content signals carry a plurality of programs coextensively in time;

second decryption information received from a place remote to the content receiver, wherein the second decryption information is encrypted using the first decryption information; and

first content received with the interface, wherein the first content is decrypted with a method related to the second decryption information,

wherein the first decryption information is based on the provisioning information.

23. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the content signals are protected by a plurality of encryption keys.

24. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 23, wherein the first decryption information includes a category key.

25. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information includes a category key.

26. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the second decryption information includes a content key.

27. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information expires after a period of time.

28. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 27, wherein the period of time is two hours, one day, one week, one month, or one year.

29. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information is uniquely encrypted for each of a plurality of content receivers in a system.

30. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, further comprising a plurality of content keys, wherein the first content is protected with one of the plurality of content keys.

31. (Original) The content receiver for protecting content that is transmitted with digital encoding as recited in claim 30, wherein the first decryption information includes a category key.